



University of Pennsylvania  
**ScholarlyCommons**

---

Departmental Papers (ASC)

Annenberg School for Communication

---

8-2008

# Consumers' Understanding of Privacy Rules in the Marketplace

Joseph Turow

*University of Pennsylvania*, [jturow@asc.upenn.edu](mailto:jturow@asc.upenn.edu)

Michael Hennessy

*University of Pennsylvania*, [mhennessy@asc.upenn.edu](mailto:mhennessy@asc.upenn.edu)

Amy Bleakley

*University of Pennsylvania*, [ableakley@asc.upenn.edu](mailto:ableakley@asc.upenn.edu)

Follow this and additional works at: [http://repository.upenn.edu/asc\\_papers](http://repository.upenn.edu/asc_papers)



Part of the [Internet Law Commons](#), [Privacy Law Commons](#), [Public Policy Commons](#), and the [Public Relations and Advertising Commons](#)

---

## Recommended Citation

Turow, J., Hennessy, M., & Bleakley, A. (2008). Consumers' Understanding of Privacy Rules in the Marketplace. *Journal of Consumer Affairs*, 42 (3), 411-424. <https://doi.org/10.1111/j.1745-6606.2008.00116.x>

Funds for this research were provided through the Annenberg Public Policy Center, University of Pennsylvania—Kathleen Hall Jamieson, Director.

This paper is posted at ScholarlyCommons. [http://repository.upenn.edu/asc\\_papers/406](http://repository.upenn.edu/asc_papers/406)

For more information, please contact [libraryrepository@pobox.upenn.edu](mailto:libraryrepository@pobox.upenn.edu).

---

# Consumers' Understanding of Privacy Rules in the Marketplace

## **Abstract**

Studies suggest the general structure of Web sites leads consumers away from demanding that online merchants take certain approaches to privacy as a condition for dealing with them. This article presents findings from a nationally representative survey showing that the absence of such a privacy marketplace can also be attributed to the public's incomplete knowledge of privacy regulations. Most respondents correctly understood that regulations regarding merchants' sharing information are domain specific. The respondents were only sporadically correct, however, regarding which domains have which rules. The study raises questions about the best approaches to education in the absence of a coherent national policy of privacy regulation.

## **Disciplines**

Communication | Internet Law | Privacy Law | Public Policy | Public Relations and Advertising

## **Comments**

Funds for this research were provided through the Annenberg Public Policy Center, University of Pennsylvania—Kathleen Hall Jamieson, Director.

# Consumers' Understanding of Privacy Rules in the Marketplace

Joseph Turow, Michael Hennessy, and Amy Bleakley

Studies suggest the general structure of Web sites leads consumers away from demanding that online merchants take certain approaches to privacy as a condition for dealing with them. This article presents findings from a nationally representative survey showing that the absence of such a privacy marketplace can also be attributed to the public's incomplete knowledge of privacy regulations. Most respondents correctly understood that regulations regarding merchants' sharing information are domain specific. The respondents were only sporadically correct, however, regarding which domains have which rules. The study raises questions about the best approaches to education in the absence of a coherent national policy of privacy regulation.

While studies consistently show that individuals are apprehensive about companies learning personal information about them, people rarely, if ever, read privacy policies or take steps to protect personal information collected during online transactions (Graber, D'Allessandro, and Johnson-West 2002; Vila, Greenstadt, and Molnar 2003). As Nehf (2007) and Pitt and Watson (2007) note, consumers do not act as if there is an online market for privacy that leads them to choose privacy-enhancing Web sites over others. Nehf concludes that the problem lies in the structure of the online world. That is, the online marketplace is organized such that consumers drop their sensitivity toward protecting their information to "pursue other goals that render privacy less salient than other attributes" (Nehf 2007, 355).

The aim of this article is not to dispute that structural reasons play a role in explaining the failure of online consumers to inquire into sites' privacy rules or to insist that sites not appropriate consumers' information. It is, rather, to present nationally representative survey findings suggesting that consumers' failure to protect their privacy online as well as offline can also be attributed to limited consumer's knowledge. Most respondents in the survey correctly understood that regulations regarding merchants' sharing information are domain specific. The respondents were only sporadically correct, however, regarding which domains have which rules. Our analysis highlights the dilemma of those who are looking for ways to encourage consumers to demand stronger privacy protections from marketers, and it suggests the importance of different levels of government involvement.

## THE DILEMMA OF MARKETPLACE PRIVACY

In the United States, state and federal law generally leaves it up to individuals to learn the rules by which firms can use their personal information and to assess their privacy risks when dealing with merchants in the online and brick-and-mortar worlds. The lack of a cohesive regulatory scheme may be partly a result of inattention and neglect by regulators, partly a belief that the open market has historically been an American tradition, and partly because marketers and marketing advocacy groups have convinced regulators that important new businesses would be harmed by an aggressive stance on marketplace privacy (Turow 2006).

Within this regulatory context, Americans appear to have a contradictory approach to the issue. Some research shows that they are wary about the ways corporations use data about them. For example, a poll by the consultancy Privacy and American Business found that fifty-six percent of Americans in 2002 (vs. thirty-four percent in 1999) believed that most companies do not "handle personal information they collect in a proper and confidential way" (Westin 2003). At the same time, research shows that people behave in the online and offline marketplace as if they do not mind giving up information about themselves. Madden et al. (2007) at the Pew Internet and American Life Project found that "most internet users are not concerned about the amount of information available about them online, and most do not take steps to limit that information." Other research notes that people rarely read privacy policies or take steps to protect the information from marketers online—and that many are willing to give up information

about themselves for gifts or other incentives (Hann et al. 2002; Jensen, Potts, and Jensen 2005; Jupiter Media Metrix 2002; Turow and Nir 2000).

One response to such findings has been to contend that “self-regulation works” and that government intervention on consumers’ behalf could limit U.S. industries’ competitiveness as well as the growth of the Internet. Westin (2003) contends that despite their worries, consumers can correctly evaluate the costs and benefits of giving out personal information. Westin’s argument suggests that consumers understand the privacy rules of the marketplace well enough to make informed decisions.

Some analysts disagree, arguing that the market in which consumers make choices is not an optimal one for information privacy. It is not a market where they can apply the skepticism they hold regarding collection of their information, learn the information they need to interact with merchants, and bargain with them about the data they want to give out. Pitt and Watson (2007) see the relationships between government data needs, corporate data needs, and technological change as making a privacy market impossible. Markets, they note, “require a certain level of stability to operate effectively” (374). While they take a broad view of forces militating against a unified privacy regime, Nehf (2007) focuses on the factors that lead people not to understand how to protect or negotiate their privacy. He notes that a variety of features companies build into Web sites discourage people from policing their online privacy. Among the factors he says discourage people from taking steps to protect their privacy are:

- obtuse and noncommittal privacy policies that make it difficult for people to know what information a site collects and how it will be used;
- voluntary privacy seals that do not properly signal strong privacy practices so that people will privilege those sites over others;
- lax accountability procedures on Web sites so that people have no idea when a privacy breach occurs; and
- companies falsely framing their Web sites as having strong privacy policies to take advantage of consumers’ psychological predisposition to believe the claim to overcome the time constraints and high cognitive effort required to evaluate privacy policies.

Nehf’s focus on Web sites resonates with literature not just in the area of online commerce but also in the areas of health and finance (e.g., Anton et al. 2003; Anton and Earp 2004; Goldman, Hudson, and Smith 2000). According to this perspective, consumers lack the knowledge or inclination to deal properly with privacy issues because of features of the online world and particularly aspects of Web sites. This structural view is persuasive, but partial. It emphasizes awareness of privacy rules as contingent on people’s interactions with Web sites. In doing so, it neglects to consider that people encounter descriptions or implications of privacy rules through the general information and news environment. The press fairly frequently presents stories about the stealing and accidental release of customer information. Credit card companies by law must regularly send privacy policy notices to their customers (The Gramm-Leach-Bliley Act of 1999—P.L. 106-102, §503, 113 Stat. 1439), and the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191, §1173, 110 Stat. 2024-26) requires medical caregivers to tell patients the conditions under which they guard and/or share personal information. One view of these requirements is that they are difficult if not impossible to understand, a situation that might mislead consumers into thinking that their information is protected from cross-company sharing more than it really is (Turow 2003). Juxtaposed to these press stories, the very presence of the privacy notices and their comforting accompanying letters about the protection of consumer data may suggest an entirely different nature of privacy regime to their recipients.

Developing practical expertise regarding information privacy is not easy. Unlike regulators in other jurisdictions—those in the European Union, for example—lawmakers in the United States have not provided citizens with a coherent perspective through which they can understand how merchants must approach the privacy of their personal information (Langenderfer and Cook 2004). The consequence is a patchwork of regulations that reflects particular disconnected struggles over what information privacy

should mean in certain areas of commerce—for example, the health and financial services industries—as well as in merchants’ involvement with children younger than thirteen years. Apart from these exceptions, companies are generally *unconstrained* in their use of data for business purposes. They can take, use, and share personally identifiable data: information linked to individuals’ names and addresses. They can also create, market, and sell detailed profiles of people whose names they do not know but whose interests and lifestyles they statistically infer from their activities online and offline (Pack 2000; Solove and Rotenberg 2003).

Despite the complexity of this regulatory environment, our findings based on a survey of adult Internet users suggest that Americans do have frameworks of knowledge regarding privacy in the marketplace. It is what they know, and especially what they believe they know, that is problematic.

## METHODS AND MEASURE

### Survey

We examined the nature of Americans’ knowledge regarding privacy as part a larger study of Americans’ knowledge of the laws regarding a company’s right to collect information about them online or offline and to charge them and others different prices for the same items at the same time. Because of our interest in people’s relationships to both the online and the offline selling environments, we focused on U.S. adults who use the Internet. We included people aged eighteen years or older in our study if they said yes to the question, “Have you used the Internet in the past month at home, work, or anywhere else?”

ICR/International Communication Research of Media, Pennsylvania, collected the survey data from February 8 to March 14, 2005, using a nationally representative random digit dial sample to screen households for adults aged eighteen or older. The telephone interviews, which averaged twenty minutes, were completed with a nationally representative sample of 1,500 adults. The process involved computer-assisted telephone interviewing, which ensures that questions follow logical skip patterns and that attitude statements are automatically rotated, eliminating question position bias. Using the American Association of Public Opinion Research RR3 method, a standard for this type of survey, the overall response rate for this study was 58.4%. The margin of error for percentages was  $\pm 2.5\%$  at the 95% confidence level, although the margin of error was higher for subgroups.

### Measures

Table 1 shows the item set analyzed here. Items A–G refer to collecting and disclosing personal data. We analyzed these items in two different ways. First, we recoded the responses to reflect the correspondence between the correct answer and the respondent’s answer. When coded this way, the items represent a knowledge index about information collection and disclosure by online and offline retailers. We also analyzed the respondent’s unmodified true or false answers as reflecting a belief index about collection and disclosure behavior by online and offline retailers. Put another way, the first analysis of items A through G takes the “correctness” of the survey responses into account and treats the items as reflecting a potential knowledge structure, while the second analysis of items A through G ignores the correctness of the survey responses and treats the items as reflecting a belief index.

## FINDINGS

### Sample Characteristics

Table 2 provides a summary snapshot of the survey participants. Women slightly outnumbered men; seventy-three percent of participants designated themselves as non-Hispanic white and eight percent called themselves non-Hispanic blacks. Hispanics (white and black) comprised about ten percent of the

TABLE 1

*Knowledge Items with Correct Answers and Survey Percentage Correct (N = 1500)*

Knowledge Items on Collecting and Disclosing Personal Data	Correct Response	% Correct
A. Companies today have the ability to follow my activity across many sites on the Web.	TRUE	83
B. A Web site is allowed to share information about me with affiliates without telling me the names of the affiliates.	TRUE	51
C. When I subscribe to a magazine, by law that magazine cannot sell my name to another company unless I give it permission.	FALSE	48
D. My supermarket is allowed to sell other companies information about what I buy.	TRUE	36
E. When I give money to charity, by law that charity cannot sell my name to another charity unless I give it permission.	FALSE	28
F. A video store is not allowed to sell information about the titles I have rented.	TRUE	29
G. When a Web site has a privacy policy, it means the site will not share my information with other Web sites or companies.	FALSE	25

sample, Asian Americans made up three percent, and Native Americans comprised about one percent. About sixty percent were younger than forty-five years, fifty-seven percent were married, and forty-four percent had children younger than 18 years. Most had at least some higher education, and while a substantial percentage said their household brought in more than \$75,000 annually, a firm claim about the sample's income distribution is difficult because seventeen percent of the population refused to reveal it. Other data collected included Internet use, self-reported computer and Internet skills, and shopping patterns; these variables are discussed below.

#### Understanding Merchants' Rights to Share Personal Information

The first analysis of items A through G in Table 1 treated them as measures of *knowledge* of data collecting and disclosing policies. Item A was the easiest to answer; eighty-three percent knew that companies have the ability to follow their activity across many sites on the Web. A far smaller percentage answered the other knowledge areas correctly. Around one-half correctly answered B and C—about Web sites and magazines sharing personal information. Only thirty-six percent knew the answer to the question about supermarkets and personal information; fewer than thirty percent correctly answered the questions about charities and video stores' policies. Item G was the most difficult. Only twenty-five percent knew that the statement “When a Web site has a privacy policy, it means the site will not share my information with other Web sites or companies” was false.

To determine whether the items in the knowledge and belief indices were one dimensional, we used the KR20 statistic, a version of *alpha* appropriate for dichotomous data (Streiner 2003) and Mokken scaling. Mokken scaling assumes that unidimensionality of the items is defined by their ranking along an unobserved “difficulty” dimension such that all items after the initial failure are also failed and all items before the initial failure are passed, a “Guttman pattern” of responses (Ringdal et al. 1999, 27). If the item scale using this definition, then the scale score implies that the respondent passed the items less than or equal to the observed score and failed all difficulty-ranked items greater than the value of the observed score.

TABLE 2

*Characteristics of Survey Respondents (N = 1,500)*

Respondent Characteristics	% <sup>a</sup>
<i>Gender</i>	
Male	48
Female	52
<i>Age (years)</i>	
18–34	37
35–44	22
45–54	18
55–64	10
65+	12
No answer	2
<i>Race and ethnicity</i>	
White non-Hispanic	73
White Hispanic	9
Black non-Hispanic	8
Black Hispanic	1
Asian American	3
Native American	1
Other	1
No answer	4
<i>Education</i>	
Less than high school graduate	8
High school/tech school graduate	31
Some college	27
College graduate or more	34
No answer	1
<i>Family income</i>	
Less than \$40K	26
\$40K but less than \$75K	29
\$75K but less than \$100K	13
\$100K+	14
Do not know/no answer	17
<i>Parental status</i>	
A parent of child younger than eighteen years	44
Not a parent of child younger than eighteen years	54
No answer	2

<sup>a</sup>When the percentages fail to sum to 100%, it is because of rounding error.

Analysis of the relationships among the responses to the seven statements indicated a unidimensionality that conforms to a Guttman scale. The KR20 value was .73, which is high internal

consistency, especially for test items as opposed to psychological ones. The Mokken scaling module in stata estimated a Loevinger's  $H$  (a measure of scalability) of .41 for the seven items, which is considered a "moderate" scale (Mokken, 1971). Overall, the average for the knowledge scale index was 3.22 items correct ( $SD = 1.99$ ). Because the scale had a difficulty-ordering pattern, the correct items tended to be A, B, and C. Much smaller proportions of respondents knew the answers to D through G. Only 6.3% of all the respondents knew the correct answers to all seven questions. These results imply that moving from items A to G, if a respondent answered a question correctly, she/he was likely to know the correct answer to the easier questions before it. This scaled response pattern applied (e.g., showed the same ordering of items) even when background characteristics (e.g., gender, ethnicity, and age) were taken into account.

A plausible explanation for the respondent's knowledge can be linked to their education level: either they may have been taught the correct answers or their education may have provided them with the tools or skills to develop sophisticated knowledge frameworks. Education level was associated with the total knowledge score,  $F(4, 1842) = 27.02, p < .05$ . Those with graduate education had the highest knowledge score (mean = 3.85,  $SD = 2.06, N = 306$ ), while those with less than a high school education had the lowest (mean = 1.81,  $SD = 1.64, N = 31$ ).

In addition to differences by educational level, there were statistically significant differences in the average number of correct items by other respondent characteristics. When age was classified into four categories, the average knowledge score was significantly different between the age categories,  $F(3, 1484) = 9.64, p < .05$ . Average values on the knowledge scale were highest for the fifty- to sixty-four-year-old group (mean = 2.9,  $SD = 1.95, N = 142$ ) and lowest for the eighteen- to twenty-nine-year-old group (mean = 2.67,  $SD = 1.8, N = 238$ ). There was also a gender difference in knowledge; males' average score was 3.47 ( $SD = 1.95$ ), while females averaged 3.01 ( $SD = 2.02$ ), a statistically significant difference between means ( $t = 4.35, p < .05$ ). Finally, the questionnaire collected data on the respondents' self-reported "abilities to go online or navigate the Internet." The levels of assessment were "a beginner" ( $N = 187$ ), "an intermediate user" ( $N = 638$ ), "an advanced user" ( $N = 506$ ), and "an expert user" ( $N = 167$ ). Using these categories, we found that the knowledge score was significantly related to the respondent's self-assessment of skill,  $F(3, 1497) = 25.5, p < .05$ . The average values for the four skill groups (from least to most skilled) were 5.25 ( $SD = 3.05$ ), 6.50 ( $SD = 3.47$ ), 7.27 ( $SD = 3.29$ ), and 8.04 ( $SD = 3.60$ ).

The scaled array of the responses indicated a patterned set of responses; people who knew the right answers to certain statements about domains tended to be correct on statements regarding other domains. Yet the proportions of people who knew any of the statements below C were lower—often substantially lower—than 40%. People tended to state that companies in certain domains are allowed to share personal information but companies in other domains are not. So, for example, while fifty percent knew that the law does not protect the sharing of their personal information when it comes to the Web, only thirty-six percent also knew that this lack of protection applies to supermarkets and only twenty-eight percent knew that it applies to charities. If they believed that all domains fall under the same regulations, these percentages should be the same. Rather, such inconsistencies regarding firms' rights to share information across the range of domains indicate that most people believe that information-sharing rules are specific to particular merchant domains.

This conclusion was corroborated when we attempted to scale items A through G as a set of beliefs. Here, we ignore the correctness of the response and just analyze the intercorrelations between the items. As a set of beliefs, there was no pattern to the true or false responses at all: the KR20 was -.19. The items treated as beliefs were also not scaleable as to difficulty; Loevinger's  $H$  was -.035. Most strikingly, we found only a small (although significant) positive correlation between a respondent's score on the correct answer index and an index constructed from the summed belief items; the polychoric correlation between the two variables was .08 ( $N = 1,500, p = .004$ ). This small correlation highlights the respondents' lack of agreement about what domains are prohibited from sharing their private information and what domains are allowed to do so.

Our conclusion is that a small proportion of Internet-using American adults have a highly sophisticated knowledge framework regarding marketplace privacy. That segment has learned the



regulations that allow it to correctly distinguish the circumstances in which merchants have the right to share information in different marketplace domains. A slightly larger proportion (the ones who knew all but the video-store answer) holds a less sophisticated, but nevertheless typically correct, framework. From our data, we cannot tell whether this framework reflects actual knowledge of every specific marketplace domain except for video stores or whether it is based on a general assumption (wrong only in the video-store case) that the government always allows merchants to share people's private information. It is clear from the data that the large majority of Internet-using adults understand that regulations regarding merchants' sharing information are domain specific. At the same time, that majority was only sporadically correct regarding the true-false statements. The general picture of the population at large is one of the selective and limited knowledge about where in the marketplace one might find merchants who are legally allowed to share customers' personal information without their consent.

## DISCUSSION

People who believe that banks send customers e-mails asking them to verify their accounts leave themselves open to "phishing," whereby thieves using e-mail persuade customers to give them private banking information and then steal their money. In our sample of Internet-using American adults, forty-nine percent did not know this fact about the online world. The misunderstanding helps explain the \$630 million that the Consumer Reports National Research Center estimates was stolen by this method through September 2006 (Consumer Reports 2006). Unfortunately, phishing is only one facet of Americans' ignorance of activities and rules relating to use of their private information. While a great majority of Americans know that companies have the ability to follow them across sites on the Web, far fewer know important facts about how merchants can take their information, about their recourse to complain if credit-related errors arise as a result of data collection, or that many types of merchants online and offline have the legal right to share information about them with other organizations even if they do not ask their permission.

These findings and others from this study broaden the concerns that observers such as Pitt and Watson (2007) and Nehf (2007) have regarding the structural impediments to privacy demands of Web sites by the public. The public's knowledge of the rules of privacy in the marketplace is clearly absent not just online but also offline and across a variety of for-profit and nonprofit entities. Our findings suggest that this ignorance goes beyond the failure to learn about specific privacy details at the point of individuals' interactions with merchants. It is rooted in a broader difficulty: the combination of a generally correct awareness of the fragmented nature of privacy regulation linked to frequent mistakes about actual facts of those regulations.

In the face of a misunderstanding of privacy regulations in the marketplace, a two-pronged approach of education and mandatory labeling may be required to make Americans aware of the data collection environment that surrounds them. Studies of the impact of the 1990 Nutrition Labeling and Education Act (e.g., Burton and Biswas, 1993; Burton, Creyer, and Huggins 2006; Burton, Garretson, and Velliquette, 1999) provide an interesting parallel. They suggest that education *and* mandatory labeling are both necessary in order to encourage consumer interest in, understanding of, and use of data that affect them but of which they have been unaware. Reflecting on a multimethod study of consumer responses to nutrition labeling, Balasubramanian and Cole (2002, 126) summarize that "Consumers care about nutrition information, but with two important nuances: First, they appear to rely on simple heuristics to collect nutrition information, that is, using the easy-to-digest information in descriptor terms or nutrition claims rather than the more comprehensive information in the Nutrition Facts panel .. Second, they appear to care more about certain types of nutrition information (negative types)." Balasubramanian and Cole (2002, 124) noted that "both nuances may yield suboptimal nutrition choices," and this conclusion reinforces their suggestion that public policy officials should increase education about nutrition and nutrition labeling along with the required labeling.

Our findings regarding marketing and privacy suggest that, as with nutrition information, consumers rely on simple heuristics. That is why in the absence of a unified national philosophy about

marketplace privacy to teach the rules in a logical manner, the best approach for educating Americans on the subject may well be to streamline the discussion of the regulations. Schools, community organizations, and media should describe privacy rules in ways that explicitly contradict the claims of customer choice implied by the corporate disclosures that people get in the mail and read on the Web. While there are some specific exceptions to merchant power over customer data, in most domains of U.S. commerce, merchants have the right to share customers' personal information without their permission and the right to manipulate data to suit business aims without telling their customers. Encouraging a consumer orientation that emphasizes skepticism and assumes a lack of privacy protections may well lead them to be more correct than mistaken on this subject.

This sort of privacy education should, however, be accompanied by labeling requirements. The reason centers on the complexity, ambiguity, and lack of transparency that consumers confront in relation to privacy. Inaccurate knowledge frameworks may well be reinforced by structural features of the retail experience that Nehf (2007) clearly describes. In supermarkets, for example, our finding that people's incorrect belief that the stores are not allowed to sell their information may be reinforced by the emphasis on speed at checkout counters. The fast-paced nature of the interaction at checkout counters makes it improbable that discussions will take place about the data collected with frequent shopper cards. The same type of structural reinforcement of inaccurate knowledge likely takes place with a Web site's link to its privacy policy. The very existence of the link may discourage people from reading the policy by exploiting their inaccurate knowledge regarding rules that govern merchants' use of information. Recall our finding that only twenty-five percent of respondents correctly said "false" to the statement "when a Web site has a privacy policy, it means the site will not share my information with other Web sites or companies." At the point of entry, then, individuals are inclined to believe that the law protects them and that the privacy policy merely states that. Our finding suggests that the label "privacy policy" is effectively even if not intentionally deceptive when used on a site that does not handle information in the way that a majority of Americans believe the label signifies. One response to this situation would be for the Federal Trade Commission to require a nondeceptive tag, such as "using your information," for areas of Web sites where rules for handling visitor information are described.

Businesses generally do not have sufficient incentive to implement this sort of transparency online or offline (Nehf 2007; Turow 2006). In the interest of encouraging a marketplace for privacy guidelines, it may therefore be up to the federal government to require posting of data collection policies that follow an orderly, predictable, and understandable template at the entry to all online and offline businesses. These two approaches—educating people in privacy frameworks that are accurate and requiring merchants to post information where they shop in ways that will allow them to use those frameworks—may go a long way toward establishing a beneficial marketplace for information privacy.

## REFERENCES

- Anton, Annie and Julie B. Earp. 2004. A Requirements Taxonomy for Reducing Web Site Privacy Vulnerabilities. *Requirements Engineering*, 9 (3): 169–185.
- Anton, Annie, Julie B. Earp, Davide Bolchini, Qingeng He, Carlos Jensen, and William Stufflebeam. 2003. The Lack of Clarity in Financial Privacy Policies and the Need for Standardization. North Carolina State University Technical Report #TR-2. [http://66.102.1.104/scholar?hl=en&lr=&q=cache:7Y0Lck1RWWIJ:www.theprivacyplace.net/papers/glb\\_secPriv\\_tr.pdf+](http://66.102.1.104/scholar?hl=en&lr=&q=cache:7Y0Lck1RWWIJ:www.theprivacyplace.net/papers/glb_secPriv_tr.pdf+). (Accessed July 8, 2008).
- Balasubramanian, Siva K. and Catherine Cole. 2002. Consumers' Search and Use of Nutritional Information: The Challenge and Promise of the Nutrition Labeling and Education Act. *Journal of Public Health*, 66 (3): 112–127.
- Burton, Scot and Abhijit Biswas. 1993. Preliminary Assessment of Changes in Labels Required by the Nutrition Labeling and Education Act of 1990. *Journal of Consumer Affairs*, 27 (1): 127–144.
- Burton, Scot, Elizabeth Creyer, and Kyle Huggins. 2006. Attacking the Obesity Epidemic: The Potential Health Benefits of Providing Nutrition Information in Restaurants. *American Journal of Public Health*, 96 (9): 1669–1675.
- Burton, Scot, Judith A. Garretson, and Anne M. Velliquette. 1999. Implications of Accurate Usage of Nutrition Facts Panel Information for Food Product Evaluations and Purchase Intentions. *Journal of The Academy of Marketing Science*, 27 (4): 470–480.
- Consumer Reports. 2006. State of the Net, 2006. September. [http://www.consumerreports.org/cro/electronics-comp-uters/online-protection-9-06/state-of-the-net/0609\\_online-prot\\_state.htm](http://www.consumerreports.org/cro/electronics-comp-uters/online-protection-9-06/state-of-the-net/0609_online-prot_state.htm). (Accessed November 13, 2007)
- Goldman, Janlori, Zoe Hudson, and Richard Smith. 2000. *Privacy: Report on the Privacy Policies and Practices of Health Web Sites*. Oakland, CA: California HealthCare Foundation. Accessed <http://www.chcf.org/topics/view.cfm?itemID=12497>. (Accessed November 11, 2007)

- Graber, Mark, Dona M. D'Allessandro, and Jill Johnson-West. 2002. Reading Level of Privacy Policies on Internet Health Web Sites. *Journal of Family Practice*, 51 (7): 642–645.
- Hann, Il-Horn, Tom Lee, Kai-Lung Hui, and I.P. Pug. 2002. Online Information Privacy: Measuring the Cost-Benefit Trade-Off. *Proceedings of the Twenty-Third International Conference on Information Systems*. [http://www.comp.nus.edu.sg/~ipng/research/privacy\\_icis.pdf](http://www.comp.nus.edu.sg/~ipng/research/privacy_icis.pdf). (Accessed July 8, 2008)
- The Health Insurance Portability and Accountability Act of 1996, Public Law No. 104–191, §1173, 110 Stat. 2024–26.
- Jensen, Carlos, Colin Potts, and Christian Jensen. 2005. Privacy Practices of Internet Users: Self-Reports versus Observed Behavior. *International Journal of Human-Computer Studies*, 63: 203–227.
- Jupiter Media Metrix. 2002. *Seventy Percent of US Consumers Worry About Online Privacy, But Few Take Protective Action*. Press Release, June 3.
- Langenderfer, Jeff and Don Cook. 2004. Oh, What a Tangled Web We Weave: The State of Privacy Protection in the Information Economy and Recommendations for Governance. *Journal of Business Research*, 57 (7): 734–747.
- Madden, Mary, Susannah Fox, Aaron Smith, and Jessica Vitak. 2007. *Digital Footprints: Online Identity Management in the Age of Transparency*. Washington, D.C.: Pew Internet and American Life Project, 2007. <http://www.pewinternet.org/>. (Accessed July 8, 2008)
- Mokken, Robert. 1971. *A Theory and Procedure of Scale Analysis*. The Hague, The Netherlands: Mouton.
- Nehf, James P. 2007. Shopping for Privacy on the Internet. *Journal of Consumer Affairs*, 41 (2): 351–365.
- Pack, Todd. 2000. Law Too Weak to Help Much; Some Statues Attempt to Protect Your Privacy, but Advocates Say They Are Filled with Loopholes. *Orlando Sentinel*, September 24, A13.
- Pitt, Leyland F. and Richard T. Watson. 2007. An Ecosystem Perspective on Privacy. *Journal of Consumer Affairs*, 41 (2): 365–375.
- Ringdal, Kristen, Gerd Ringdal, Stein Kaasa, Klaus Bjordal, Marcus Wisløff, Ian Sundstrøm, and Marianne Hjermstad. 1999. Assessing the Consistency of Psychometric Properties of the HRQoL Scales within the EORTC QLQ-C30 across Populations by Means of the Mokken Scaling Model. *Quality of Life Research*, 8 (4): 25–43.
- Solove, Daniel and Marc Rotenberg. 2003. *Information Privacy Law*. New York: Aspen Publishers.
- Streiner, David. 2003. Starting at the Beginning: An Introduction to Coefficient Alpha and Internal Consistency. *Journal of Personality Assessment*, 80 (1): 99–103.
- Turow, Joseph. 2003. *Americans and Online Privacy: The System is Broken*. Philadelphia, PA Annenberg Public Policy Center. [http://www.annenbergpublicpolicycenter.org/04\\_info\\_society/2003\\_online\\_privacy\\_version\\_09.pdf](http://www.annenbergpublicpolicycenter.org/04_info_society/2003_online_privacy_version_09.pdf). (Accessed July 8, 2008) ———. 2006. *Niche Envy: Marketing Discrimination in the Digital Age*. Cambridge, MA: MIT Press.
- Turow, Joseph and Lilach Nir. 2000. *The Internet and the Family 2000: The View from Parents, the View From Kids*. Philadelphia, PA: Annenberg Public Policy Center.
- Vila, Tony, Rachel Greenstadt, and David Molnar. 2003. Why We Can't Be Bothered to Read Privacy Policies. In *ACM International Conference Proceeding Series*, edited by Norman Sadeh, Vol. 50, pp. 403–407. New York: ACM Press.
- Westin, Allen. 2003. Social and Political Dimensions of Privacy. *Journal of Social Issues*, 59 (3): 431–453.